Office of Protective Services

Counterintelligence
Counterterrorism Division

"Detect, Deter, and Neutralize"

Prepared by
NASA OPS CI/CT
Division
SSC CI Office

NASA Counterintelligence

Counterintelligence Executive Briefing

February 5, 2016

OPM BREACH: What is the Risk?

Counterintelligence Executive Briefing

This Counterintelligence Executive Briefing (CIEB) was prepared by the NASA SSC Counterintelligence (CI) Office and is designed to educate the NASA work force about counterintelligence/counterterrorism activities relevant to NASA. To report suspicious behavior, contact the NASA CI Office at 228-688-1967.

EXECUTIVE SUMMARY

This CIEB provides NASA employees and contractors with information about their vulnerabilities related to the Office of Personnel Management (OPM) breach, or any other breach where personal data was stolen, like the recent breach at Target Stores. This CIEB provides valuable information detailed by CNN Justice Reporter Evan Perez, on January 19, 2016, article titled, "New campaign warns of espionage in wake of OPM breach."

THE BREACH

For the rest of their lives, 22 million Americans will have to think twice about strangers who try to befriend them at coffee shops, at workplace conferences, or while on vacation. Could a new friend simply be a spy agency [or employee from a competing company] trying to make inroads for later exploitation? It's one of the long-lasting results of the data breach at the Office of Personnel Management, which revealed last year that hackers had stolen a vast trove of records on current and former U.S. government employees and their family members. U.S. officials believe that Chinese government hackers are behind the breach.

Bill Evanina, the nation's top counterintelligence official, is leading a new campaign to warn government employees and contractors, even those who don't deal with classified information [or have a security clearance], that partly as a result of the OPM hack they are all potential human targets by intelligence agents.

"You have an enduring threat from a counterintelligence perspective," Evanina, the National Counterintelligence Executive and director of National Counterintelligence and Security Center, told CNN in a telephone interview. "The threat is now, and it is enduring. If they decide to compromise me, they may do it now, they may do it in three years." Evanina calls the OPM breach a "watershed moment."

The documents stolen included so-called SF-86 forms, the U.S. government applications for security clearances that require prospective employees to reveal intimate personal information as part of background investigations. It's the type of information that Evanina and other officials believe likely will set the stage for foreign intelligence agents to target current and former U.S. government workers and contractors.

Evanina's agency has prepared a series of videos to help train workers about how to secure their personal information, including their interactions on social media, and how to not fall victim to hackers or foreign spies. One video being released this week focuses specifically on the threat of human targeting by foreign intelligence agents, particularly in the wake of the OPM hack.

The video depicts a low-level government analyst attending a conference and who coincidentally is befriended by a man who purports to be a fellow alumnus of the college the analyst attended. Later, the analyst's new friend -- an apparent foreign intelligence agent -- clumsily tries to get him to share work information. (This video can be seen here https://www.youtube.com/watch?v=XpqOEniQK9U&feature=youtu.be)

Evanina says he hopes to create awareness that foreign spies could use private information from the OPM hack to try to make a personal connection. The information could be used to send friend requests on social media, or to launch spear phishing emails targeting government workers. U.S. spy agencies use some of the same methods to try to target human sources in other countries. That's how Evanina knows what other countries might be trying to do to U.S. government workers and contractors.

Even after workers retire, foreign spy agencies may still find victims of the OPM breach to be attractive targets. And if the foreign spy agencies are any good at their work, it will be hard to tell when they're exploiting the data from the OPM hack. "Will we see it manifested? Probably not," Evanina said. "If a foreign intelligence service is targeting you, we're not going to know and see it until it's probably too late." The campaign makes clear that the U.S. concern isn't just about the closely held classified secrets.

"You don't have to work for the CIA or have access to the most prized information for you to be a target," said Evanina, who is an FBI agent. "Often times they go for more people with access to information that is more germane to" specific needs a foreign power is seeking. The Justice Department has brought cases involving alleged economic espionage aimed at stealing technology and proprietary information that aren't considered top national security secrets.

In 2010, a deadly fire at a high-rise renovation project in Shanghai prompted Chinese municipalities to tighten requirements for fire-proof insulation in construction projects. Two years later, the FBI arrested two Chinese nationals who tried to obtain the formula for Corning Corp's cellular-glass insulation by bribing a company employee. The Corning insulation product was a badly-needed solution to problems facing Chinese developers. Rather than buy the Corning product or develop their own alternative, the Chinese decided to steal the technology, U.S. officials contend.

NASA COUNTERINTELLIGENCE PERSPECTIVE

While the OPM breach more significantly impacts government and contract employees who have security clearances, which is not the whole story. The breach did not just include people who have completed current SF-86's with active security clearances. It also involved individuals who have **ever at any time in the past** had a security clearance and completed the SF-86. So if you were ever in the military and had a SECRET clearance, your personal information was likely obtained by Chinese Intelligence.

While this CIEB focuses on the OPM breach, it is also important to understand the risks involved with data theft attacks by criminal elements like the department store breaches. The point of this CIEB is to help NASA employees understand that by virtue of where they work, not necessarily what they do, makes them an attractive target to foreign intelligence agencies and

companies/organizations with competing interests to all of the different missions that are undertaken on NASA facilities worldwide.

It is important to understand that you are working for or supporting the U.S. government and for the world's premier space agency, both of which makes NASA and NASA employees a target for foreign intelligence services, terrorist organizations and/or criminal organizations. If you feel like you are being targeted or something just does not seem right, report that information to NASA Counterintelligence, SSC 228-688-1683. Keep your guard up. Follow security protocols no matter what.

Questions concerning this CIEB should be directed to Special Agent Ryan Reiche at the SSC CI Office (228) 688-1967.

Distribution
SSC/MAF/NSSC All Personnel

SOURCE

1. **http://www.cnn.com/2016/01/19/politics/opm-data-breach-espionage/**
2. **http://www.ncsc.gov/humantargeting.html**